AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of New York

UNITED STATES OF AMERICA
v.

Case No. 5:17-MJ-00173-ATB

DAMIAN DIAZ
Defendant.

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of October 2015 to May 2016 in the county of Onondaga in the Northern District of New York the defendant violated:

Code Section	*Offense Description*
18 USC §§1343, 1349 and	Wire Fraud and Conspiracy to Commit Wire Fraud
18 USC §§ 1956(a)(1)(B)(i) and (h)	Money Laundering Conspiracy

This criminal complaint is based on these facts:
See attached affidavit

☒ Continued on the attached sheet.

Complainant's signature

Melissa Lewis, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 04/19/2017

Judge's signature

City and State: Syracuse, NY

Hon. Andrew T. Baxter, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT OF MELISSA LEWIS

I, Melissa Lewis, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

Introduction

1. I am a Special Agent with the FBI. I have been so employed since November 2014. I am currently assigned to the Syracuse Resident Office in Syracuse, New York. Among my duties are investigating electronic crimes specifically related to wire fraud, access device fraud, and identity theft violations pursuant to Title 18, United States Code, Sections 1028, 1028A, 1029, 1343, 1349 and similar sections. I am familiar with various technologies and practices associated with the commission of such offenses.

2. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. As will be shown below, there is probable cause to believe that DAMIAN DIAZ has violated 18 U.S.C. §§ 1343, 1349 (Wire Fraud and Conspiracy to Commit Wire Fraud); and 18 U.S.C. § 1956(h) (Money Laundering Conspiracy).

4. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents, and others, as well as my personal observations and knowledge. Where statements of others are related herein, they are related in substance and in part. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a complaint and arrest warrant of DIAZ, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that DIAZ violated 18 U.S.C. §§ 1343, 1349, and 1956(h).

BACKGROUND ON ACCESS DEVICE FRAUD AS IT RELATES TO "CARDING" AND RE-ENCODED CARDS

5. Through my training and experience, I know that a common access-device fraud scheme known as "Carding" involves the trade and use of illegally obtained personal identification information (PII) and stolen account numbers through online websites or via instant messenger services. These account numbers are both a Means of Identification as defined by18 U.S.C. § 1028(d)(7)(D), and when fraudulently obtained are Unauthorized Access Devices as defined by 18 U.S.C. § 1029(e)(3)(D). "Carders" include hackers and their distributors who serve as vendors, as well as the consumers who purchase the stolen PII and account numbers and use them.

6. Through my experience I know that sellers and buyers of PII and stolen account numbers often interact and conduct transactions through instant messenger services or through websites created for the specific purpose of selling account numbers and PII. The price of account numbers varies by type and characteristics of the account and what type of corresponding PII accompanies it. A popular commodity traded by Carders is known as a "Dump," which is the electronic copy of a credit or debit card's magnetic stripe. Once the buyer provides payment, vendors are able to directly transfer stolen account information and corresponding PII to consumers directly through the instant messenger service or website. Payment is generally conducted through electronic money transfer. These methods of payment are often preferred because they readily permit international transfers. Laptop computers can be used by Carders to, among other things: access websites that sell stolen PII and account information; make online payments for stolen PII and information; and communicate directly with those offering to sell stolen PII. In my experience, once Carders purchase account numbers and PII they often save the information on their computer's hard drive or other electronic media because they may need to

edit and organize it prior to use and distribution. They also often save the information because they do not want to risk losing it if their computer crashes and be forced to buy more.

7. Once Carders obtain the stolen account numbers and PII they are able to convert them to their specific illegal use. Carders use Dumps to create counterfeit credit or debit cards. This is often accomplished through a process known as re-encoding. Re-encoding occurs when a carder obtains a stored value gift card "gift card" or credit card with a magnetic stripe and uses a device known as an "encoder," which attaches to a computer via USB or other connection, and erases or overwrites the card's magnetic stripe transferring the Dump from the computer to the card's magnetic stripe. In my experience, gift card re-encoding is often preferred to counterfeiting or altering credit cards because gift cards generally lack several security features contained on normal credit and debit cards, making it easier to alter them and yet still appear to be an authentic looking access device.

8. The credit card industry has created common standards which govern what it calls the "Payment System." The Payment System prescribes standards for how credit and debit cards are processed by merchants and what information is contained on the physical card itself. On standard credit cards, account information, including the account holder's name, account number and expiration date, are often embossed onto the front of the credit card. Pre-paid debit or gift cards are processed the same as credit cards, only have an account number and expiration date printed onto the front.

9. The Payment System terms "Card Present" transactions as those that are conducted face to face between a customer and merchant and a physical card is used to complete the transaction. A merchant processes a Card Present transaction by swiping the magnetic stripe of a customer's card through a card reader attached to a Point of Sale ("POS") Terminal. The magnetic

stripe on the card contains two commonly used "Tracks" that contain machine readable information. The account name is usually only listed on Track 1 and the account number is usually listed on both Tracks 1 and 2. According to credit card industry specifications, the embossed or printed account number listed on the front of the card must match the account numbers encoded on the magnetic stripes. As a result, a card with mismatching account numbers constitutes a Counterfeit Access Device as defined by 18 U.S.C. § 1029(e)(2). Formatting and other discretionary data is also present on both Tracks. Only Track 2 is needed to process transactions through the electronic Payment System. Some POS Terminals may read Track 1 and print the account name to the receipt. When the card is swiped, most POS systems mask all of the account information except for the last four digits of the account number, which is often printed on the receipt as well. After the payment is approved, the merchant is then required to have the customer sign an authorization slip to complete the transaction. Merchants have established anti-fraud policies, such as, for example, requiring customers to present a photo identification which matches the name listed on the card and verifying that the last four digits on the receipt match the last four digits printed on the card.

10. Many financial institutions have sophisticated fraud detection policies and mechanisms that allow them to rapidly identify compromised accounts and close them. This prevents further transactions to be processed on an account once fraud has been detected. In response to this countermeasure, Carders often use counterfeit access devices to purchase gift cards. In effect, the funds are removed from victim's account by the merchant selling the gift card to a gift card account usually operated by a separate financial institution. This added layer prevents victim financial institutions from tracing and reclaiming their funds.

11. As a result of the prevalence of re-encoded gift card fraud, many merchants have become suspicions of certain types of gift card transactions and have on occasion created their own safeguards to prevent fraud. To counter this, I have learned that Carders often attempt to spread their gift card purchases across multiple stores to avoid detection. They also generally limit the amount of gift cards they purchase at one store and may attempt to purchase other items to camouflage their actions. Carders have also been known to make multiple back to back purchases of gift cards using different re-encoded cards each time. They are also known to travel long distances, going from town to town along expressways, seeking out stores they are familiar with that sell gift cards. Carders also engage in this practice because it is difficult for store chains and law enforcement to recognize patterns in fraudulent activity when it is spread across many stores and jurisdictions. Through my experience, I know carders often use rental cars as a mode of transportation during these trips because they believe it is more difficult for law enforcement to track them.

12. Credit and debit cards can store payment information on the magnetic stripes that are part of the card. When a credit card with a magnetic stripe is used during a card present transaction, the payment information is read and used by the merchant/seller to facilitate payment from the credit or debit card account holder.

BACKGROUND OF INVESTIGATION

13. On October 1, 2015, DIAZ was stopped by police in Rochester and found to be in possession of approximately 40 fraudulent credit cards. They were embossed with his name ("Damian Diaz") but the stripes on the cards were encoded with credit card account information belonging to other individuals. DIAZ told police at that time that he had obtained the cards from

an individual named [C.W.] in Syracuse. DIAZ further admitted to police at that time that he had used at least one of the stolen credit cards to purchase gasoline.

14. In or about December 2015, Co-Conspirator #1 ("CC1"[1]) was identified by law enforcement as being involved in the use of stolen credit cards to purchase prepaid debit cards. CC1 was subsequently interviewed by authorities and admitted that he/she acquired fraudulent credit cards that were encoded with account information belonging to other individuals who had not authorized him/her to use them. CC1 also confirmed that he/she enlisted other individuals, including DIAZ, to make purchases using fraudulent credit cards.

15. On March 30, 2017, officers interviewed DIAZ. DIAZ admitted that he had purchased prepaid debit cards using fraudulent credit cards that he obtained from CC1 and that he knew the credit cards were encoded with stolen credit card numbers. He admitted that most of the prepaid debit cards ranged in value from $200 to $500. DIAZ typically was paid by CC1 approximately $200 per trip that he was swiping cards. DIAZ further admitted that the fraudulent credit cards he possessed on October 1, 2015 in Rochester were supplied by CC1 and that he (DIAZ) had lied to police when he told them that the cards were from C.W.

16. DIAZ further admitted that he used the prepaid debit cards that he purchased with fraudulent credit cards to purchase United States postal money orders. He did so in order to acquire cash and to conceal the source of the funds used to obtain the cash. DIAZ also admitted that he purchased United States postal money orders using prepaid debit cards furnished by CC1. In those instances, CC1 paid DIAZ $20 per money order that DIAZ purchased.

---

[1] The information regarding CC1 is provided to give context to the investigation. Your affiant does not believe that the information provided by CC1 is necessary to establish probable cause to believe that DIAZ has violated 18 U.S.C. §§ 1343, 1349 (Wire Fraud and Conspiracy to Commit Wire Fraud); and 18 U.S.C. § 1956 (Money Laundering Conspiracy). Accordingly, your affiant respectfully requests that the Court not rely upon it as a basis for evaluating whether there is such probable cause. If the Court believes that the information regarding CC1 is necessary to establish probable cause, your affiant can provide additional information regarding CC1's criminal history and the information furnished by CC1 to law enforcement.

17. Investigators have identified many of the U.S. Postal money orders purchased by DIAZ during December 2015 through January 2016. Based on records obtained during this investigation, DIAZ acquired or cashed at least 31 money orders totaling at least $7,949.25, which had been purchased using stolen prepaid debit cards.

18. Through my investigation in this matter, I have learned that each time that DIAZ purchased a Postal money order using stolen prepaid debit cards, a wire communication was sent from the Syracuse post office where DIAZ made the purchase to a computer server located in New Berlin, Wisconsin.

CONCLUSION

19. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that DAMIAN DIAZ has violated 18 U.S.C. §§ 1343, 1349 (Wire Fraud and Conspiracy to Commit Wire Fraud); and 18 U.S.C. §§ 1956(a)(1)(B)(i) and (h) (Money Laundering Conspiracy).

Melissa Lewis
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me

This 19th day of April, 2017,

HON. ANDREW T. BAXTER
UNITED STATES MAGISTRATE JUDGE